UNIVERSITY OF WINDSOR
ONTARIO CANADA

An Adaptive Digital Image Watermarking Technique for Copyright Protection

Mohammed J. Islam
Dept. of Elec. & Comp. Engineering

Presentation Outline

- Introduction
- Problem Statement
- Watermarking Techniques
  - Spatial Domain Watermarking
  - Frequency Domain Watermarking
- Motivation
- Proposed Method
- Experimental Results- LPF and Median
- Conclusion

Digital Media and the Internet

- Internet makes easier the transmission of digital multimedia content such as text, audio, image and video

- No quality loss
- Inexpensive copies
- Wide distribution but no control
  - Problem?

- How can Intellectual property be protected?
- How does the creator get the money?
- How to control distribution?

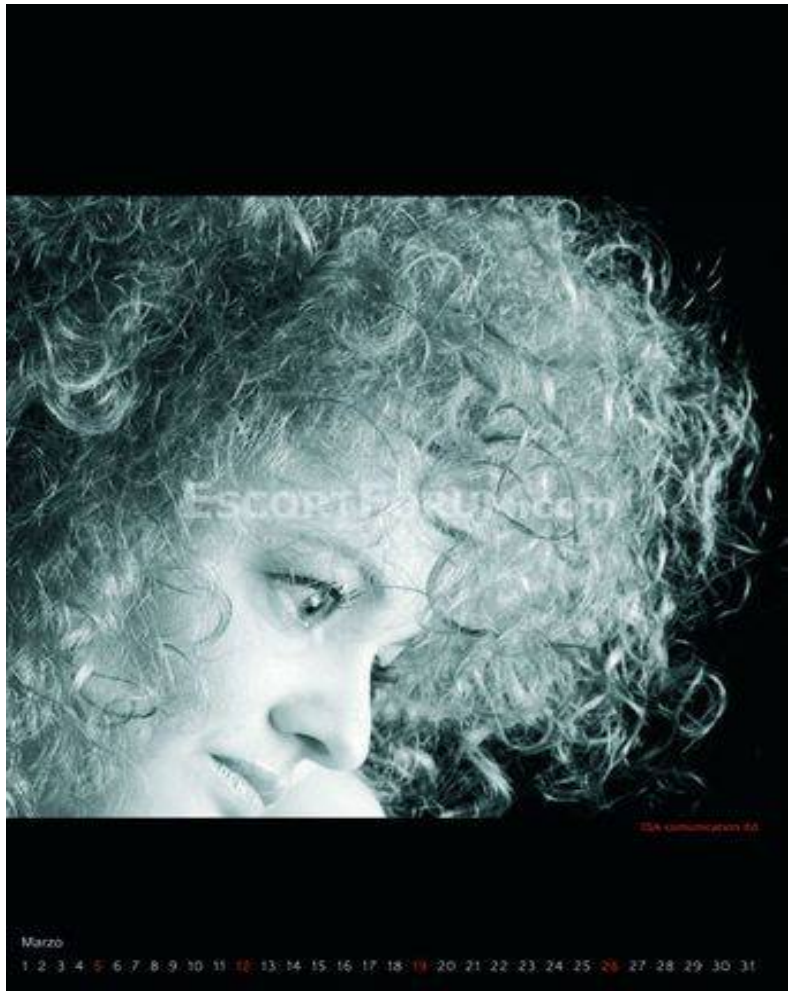
Digital Media Protection

- Traditional encryption algorithm such as DES and RSA are widely adopted.
- Digital media is encrypted into scrambled data using a predetermined encryption key (private or public)
- Correct decryption key can decrypt the encrypted data and recover original media
- What if the decrypted media is illegally distributed or copied?

- **Digital watermarking is a way of solving this issue.**

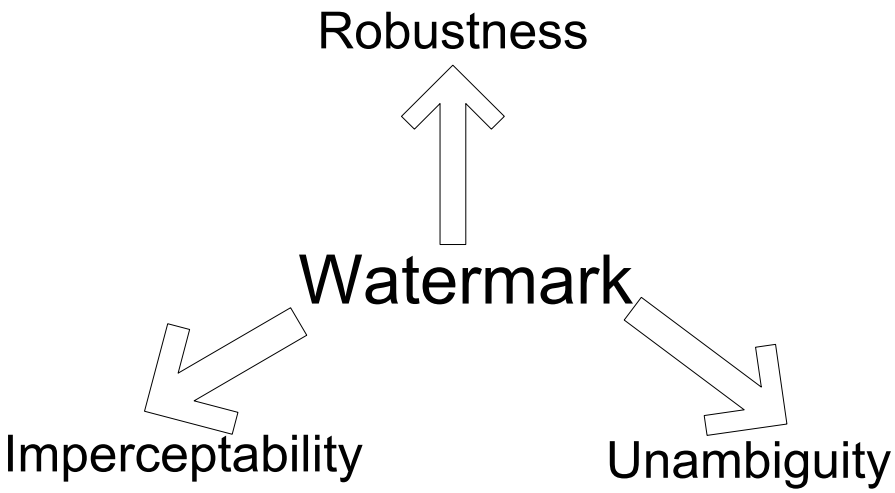
What is Watermarking?

- Embeds a mark (text or logo) into an image, text, audio and video.
- Not dependent on file format
- Visible or invisible
- Principle of digital watermarking is the robust and secret embedding of copyright information in a digital medium.



Watermark Requirements (1)

- Perceptual Transparency
  - Invisible, hidden to the human observer
- Unambiguity
  - Retrieval of watermark identify the owner.
- Robustness
  - Removal of the embedded watermark should be difficult for an attacker



Watermark Requirements (2)

- Robustness
  - Attempting to remove or destroy the watermark should produce a remarkable degradation in media quality before the watermark is lost.
  - Watermark should still be present if the watermarked media are processed by some common signal processing operations
  - Resampling, requantization, lossy compression (JPEG, MPEG, wavelet compression), linear filtering (LPF, HPF), nonlinear filtering (median filtering), geometric distortions (scaling, translation, rotation, and cropping) as well as A-to-D and D-to-A conversion

Robustness vs. Transparency

- Robustness often conflicts with transparency requirements
- To be robust a watermark should be embedded in perceptually significant regions of the host media
- To be transparent to the human observers, a watermark should be embedded in perceptually insignificant regions of the host media.
- Needs a trade-off between imperceptibility and robustness
- A balance is achieved by taking the concealment principles denoted by Human Visual System (HVS).

Human Visual System (HVS)

- HVS takes the human senses and image features into account when embedding the watermark.
- Mauro Barni suggested three rules based on the experiments:
  - Distortions are much less visible on highly textured regions than on uniform area;
  - Contours are more sensitive to noise addition than highly textured regions but less than flat areas;
  - Distortions are less visible over dark and bright regions.

How Watermark Works?

- Generate watermark based on secret key
- Transform image (e.g. DCT) or spatial domain
- Choose pseudorandom location
- Make significant yet invisible changes
- Take human visual system (HVS) into account
- Inverse Transformation

Watermark Detection

- Blind or non-blind recovery (original image required)
- Get watermark image (possibly altered)
- Extracting embedded data
- Apply error correction
- Correlation
- Decision

Spatial Domain Watermarking (1)

- Modify the intensities or color values of some selected pixels
- Simplest technique is to embed a watermark in the least significant bits (LSBs) of some randomly selected pixels
- Watermark can be easily destroyed if the watermarked image is low-pass filtered or JPEG compressed
- To increase the security, Matsui and Tanaka proposed a method to use secret key to select the locations where a watermark is embedded.

Spatial Domain Watermarking (2)

- Voyatzis and Pitas used a toral automorphism approach to scramble the digital watermark before it is inserted into an image.
- To increase the robustness of the watermark, many approaches have been proposed to modify some properties of selected pixels or blocks
- Darven and Scott proposed a fractal-based steganographic method to embed the watermark
- Wolfgang et al. reshaped an m-sequence into 2D watermark blocks, which are added and detected on a block-by-block basis.
- and many more…….

Frequency Domain Watermarking (1)

- Transforms an image into the frequency domain coefficients.
- Transformation may be Fourier transform, DCT or wavelet transforms etc.
- Watermark is then embedded in the transformed coefficients according to the perceptual significance of the transform coefficients.
- The coefficients are inverse transformed to form the watermarked image, identical to the original image
- The frequency sensitivity of the HVS can be used to ensure that the watermark is invisible and robust to any attacks

Frequency Domain Watermarking (2)

- O'Ruanaidh et. al. embedded the watermark in the phase information in the DFT domain since the phase distortion is more sensitive to HVS than the magnitude distortion. It is more robust to tampering when compared to magnitude modulation.
- Cox et. al proposed a secure spread spectrum watermarking method for embedding a watermark in the DCT domain.
- A block based DCT watermarking approach is proposed by Hsu and Wu
- and many more…….

Watermark Selection (1)

- Most of the algorithms use a serial number, a set of normally distributed random numbers, a Gaussian distribution, or an author ID as a watermark.
- A quantitative measure is required to verify the extraction result
- Usually a similarity, q, between the original watermark and extracted watermark is computed. The value of q is then tested against a threshold T.
- Determination of threshold produces another ambiguity
- Solution?

Watermark Selection (2)

- Use a visually meaningful watermark (a small image).
- Human eyes can easily verify the extracted result.
- However, a large quantity of data must be embedded into the host image if a visually meaningful image is adopted.
- The embedding algorithm must adapt its insertion strategy to accommodate a large quantity of data in the host image

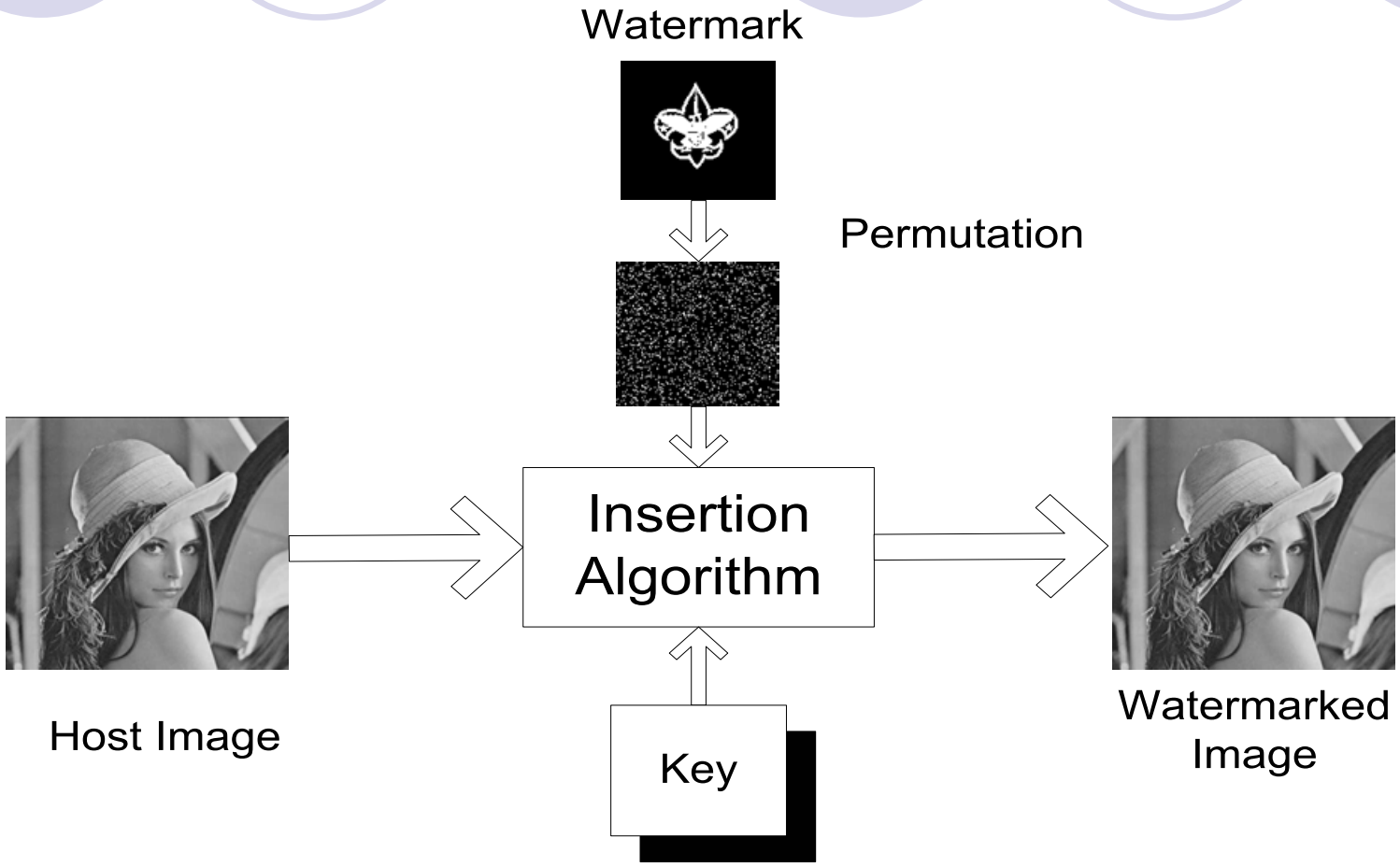
Motivation

- To provide a larger capacity for watermark insertion, a spatial domain watermarking method is used.
- Embedding a watermark in the least significant bits of a pixel is less sensitive to human eyes.
- Watermark will be destroyed if some common image operations such as low-pass filtering are applied to the watermarked image.
- So to make the embedded watermark more resistant to any attack, the watermark can be embedded in the MSBs.
- This will introduce more distortion in the host image and conflicts with the invisible requirements.

Proposed Approach

- Visually recognizable binary watermark image. So human eyes can easily identify the extracted watermark
- To meet both invisibility and robustness, the proposed method adaptively modifies the intensities of some selected pixels as much as possible and modification is not noticeable to human eyes.
- To prevent tampering or unauthorized access, the watermark is first permuted into scrambled data

Block diagram- Watermark Insertion



Watermark Insertion

Watermark Permutation

- To prevent the watermark from tampering or unauthorized access by attackers, the watermark image is first permuted to be scrambled data before insertion.

- A pseudorandom number generator is used to permute the watermark.

$$W_P = \left\{ w_P(i, j) = w\left(i', j^i\right) \middle| 0 \le i, i' < M, \middle| 0 \le j, j' < N \right\}$$

- Pixel at (i',j') is mapped to a pixel at (i,j) in a pseudorandom order. M and N are height and width of watermark image

Watermark Embedding

- The scrambled watermark image is inserted into the host image
- The embedded watermark must be invisible to human eyes and robust to most image processing operations
- To meet these requirements, a bit of pixel value(0 or 1) is embedded in a block of the host image.
- Depending on the contrast of the block, pixels in this block are adaptively modified to maximize robustness and guarantee invisibility.

Watermark Embedding Steps (1)

- The host image is decomposed into blocks of size nxn,
- The position or block for embedding is selected by pseudorandom number generator using the key K
- Step 1: Sort the pixels in block B.
- Step 2: Compute the average intensity g_{mean}, maximal intensity g_{max}, and minimal intensity g_{min} of the block.
- Step 3: Classify every pixel in B into one of the two categories,
  - b_{ij} belongs to Z_H if $b_{ij} > g_{mean}$
  - b_{ij} belongs to Z_L if $b_{ij} \leq g_{mean}$

Watermark Embedding Steps (2)

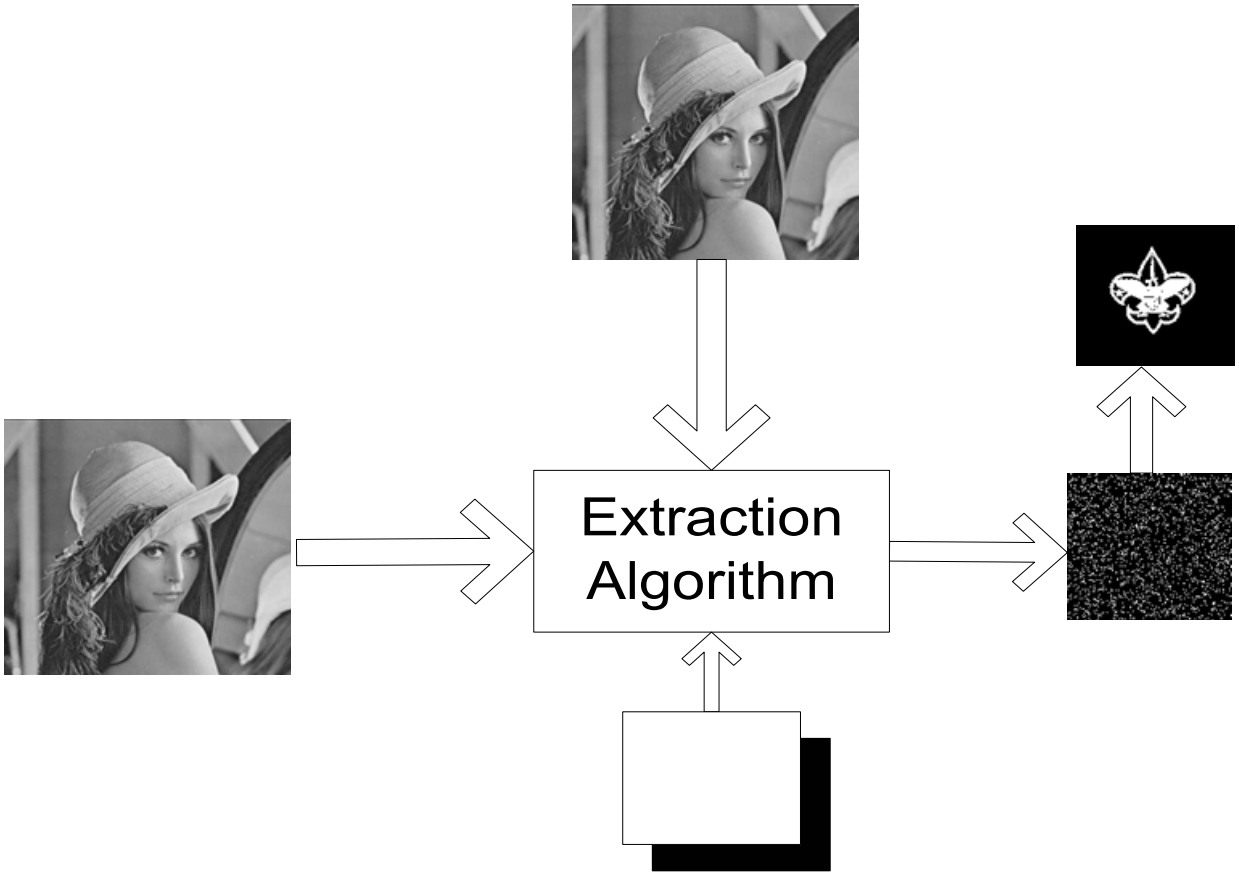
- Step 4: Compute the mean values (m_H and m_L) of these two categories
- Step 5: Define the contrast value of block B as
  - $C_B=\max(C_{min}, \alpha(g_{max}-g_{min}))$, where α, C_{min} are constant
- Step 6: Assuming the embedded value b_W is 0 or 1.
  - Modify the pixel value according to the following rules:
  - If $b_W=1$
    - $g'=g_{max}$ if $g>m_H$
    - $g'=g_{mean}$ if $m_L \le g < g_{mean}$
    - $g'=g+\delta$ otherwise

Watermark Embedding Steps (3)

- If $b_W=0$
  - $g'=g_{min}$ if $g<m_L$
  - $g'=g_{mean}$ if $g_{mean}\leq g<m_H$
  - $g'=g-\delta$ otherwise
- Where g' is the modified intensity and δ is a randomly generated value between 0 and C_B

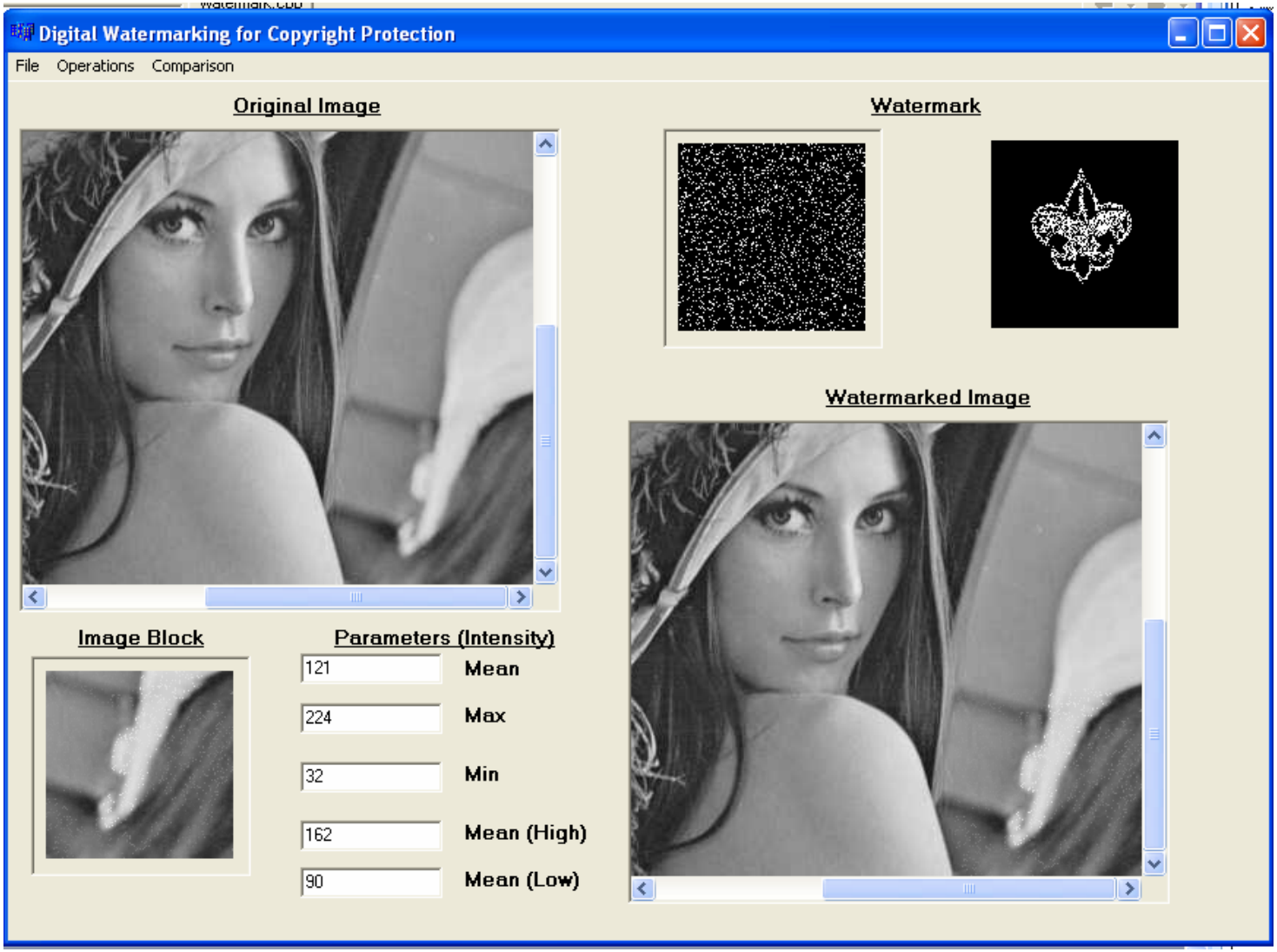
- Embedding of the watermark bit depends on the content of each block.
  - For a block of larger contrast, the intensities of pixels will be changed greatly otherwise the intensities are tuned slightly.
  - For a smooth block, the intensities of pixels will be tuned by a small randomly generated value

Block diagram- Watermark Extraction

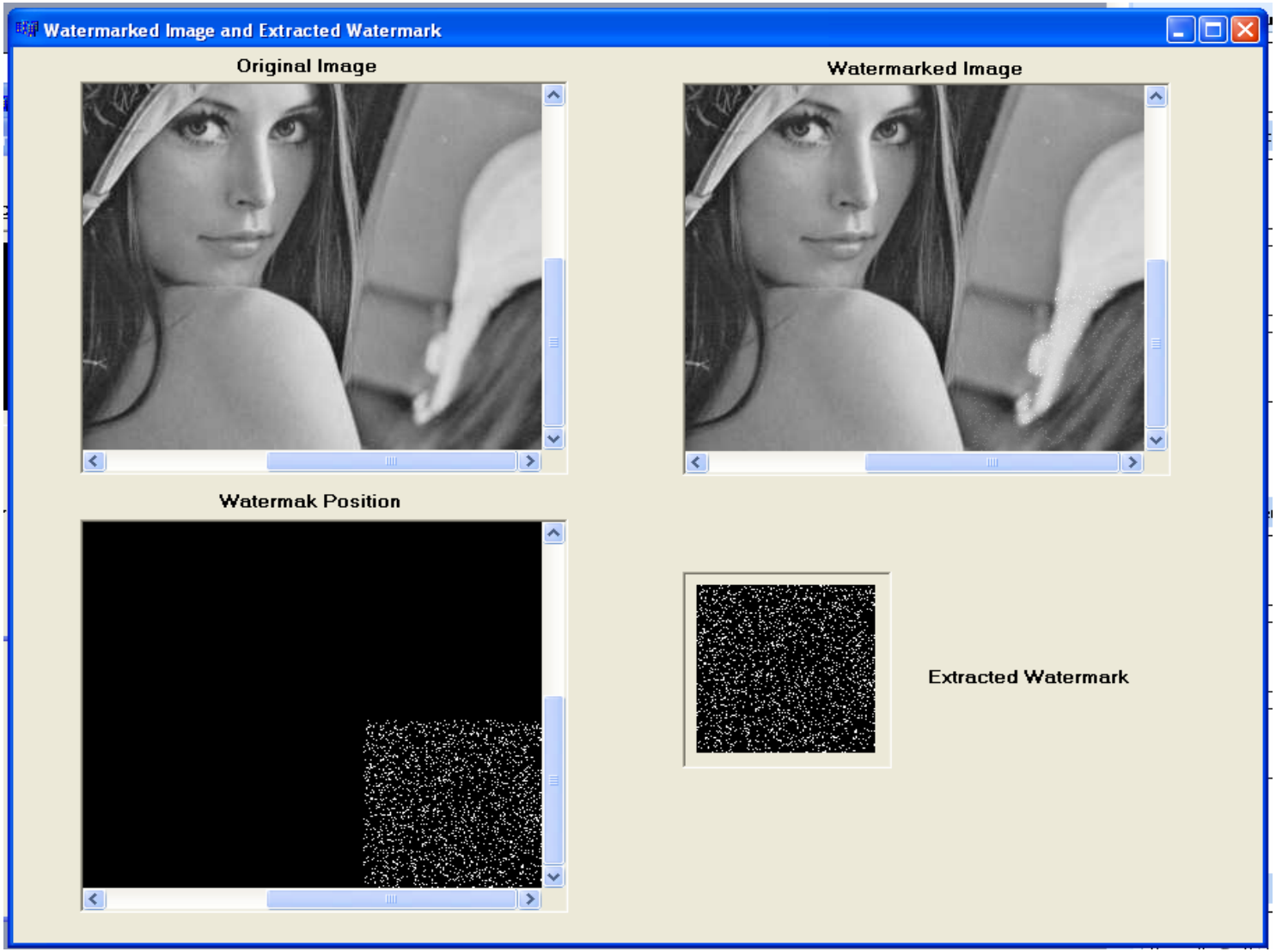


Watermark Extraction

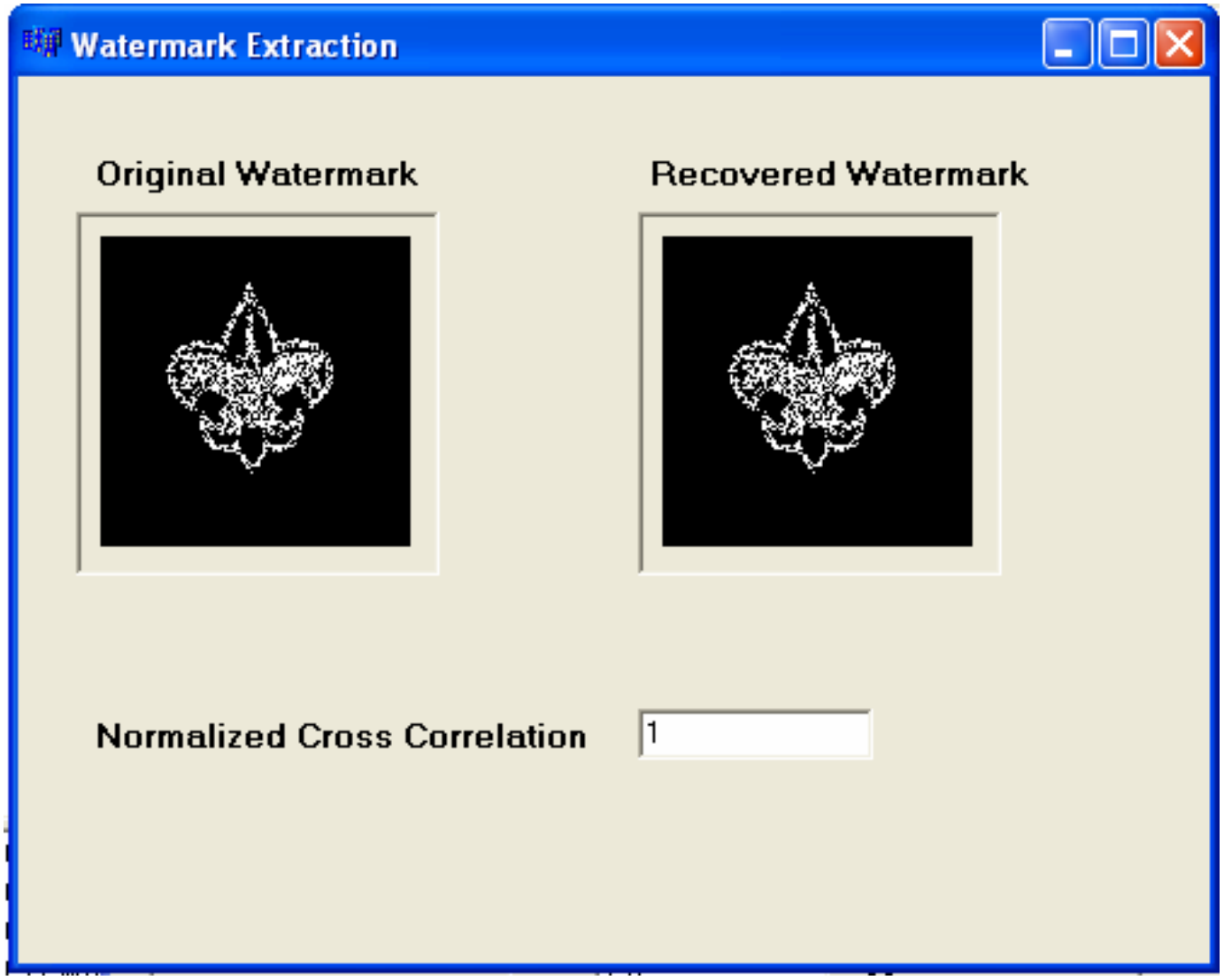
Experimental Results -Embedding



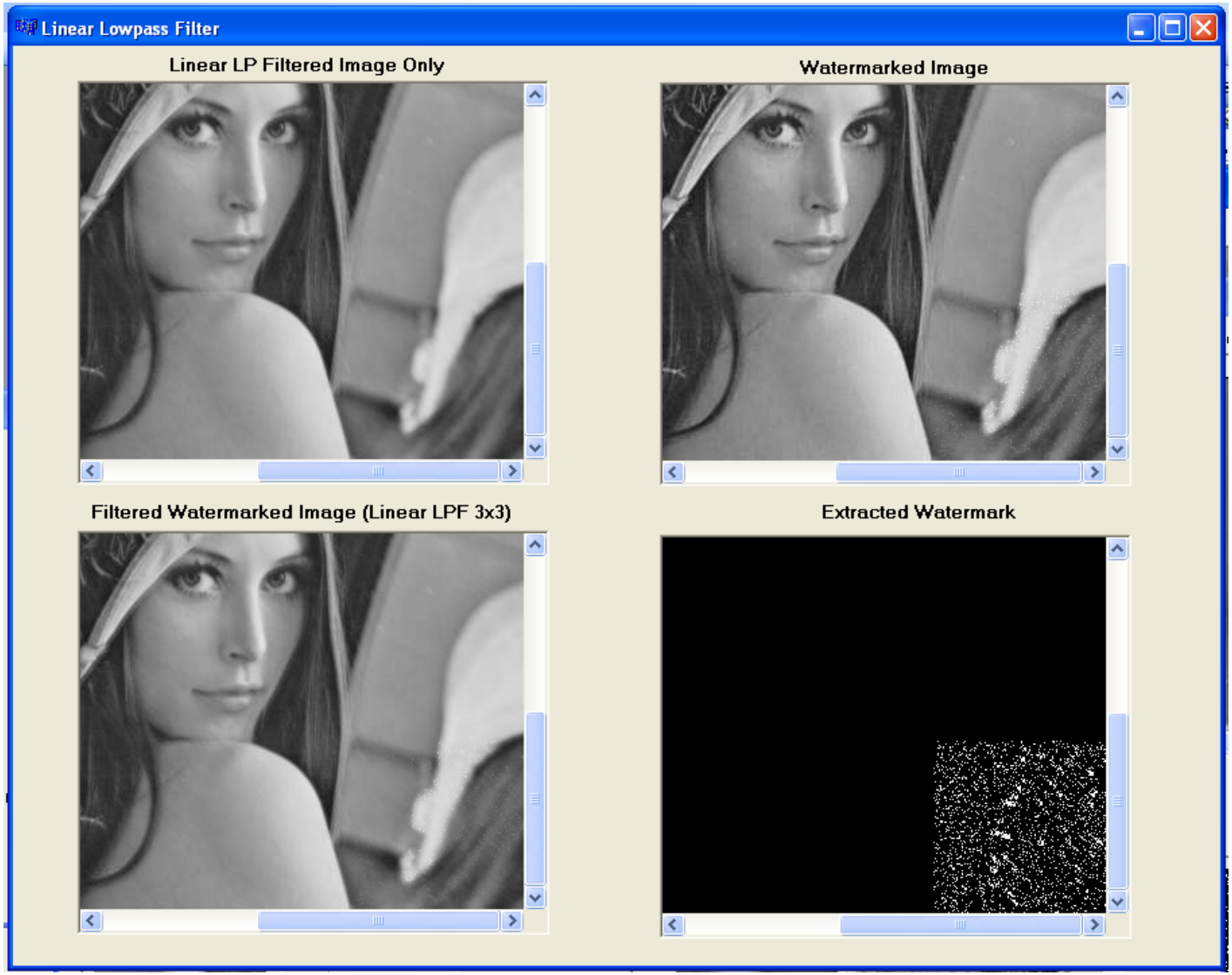
Experimental Results -Extraction



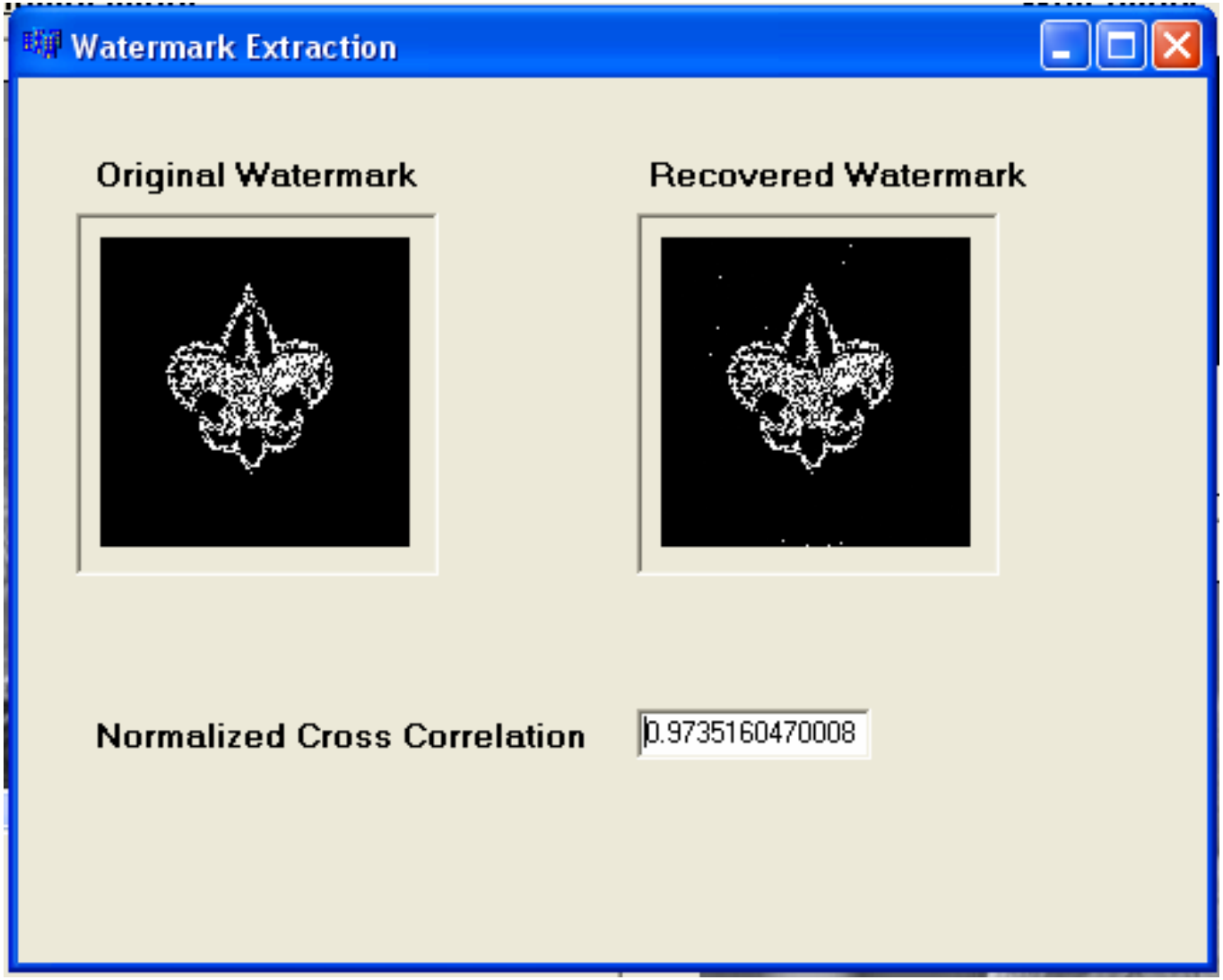
Results- Recovered Watermark-NC



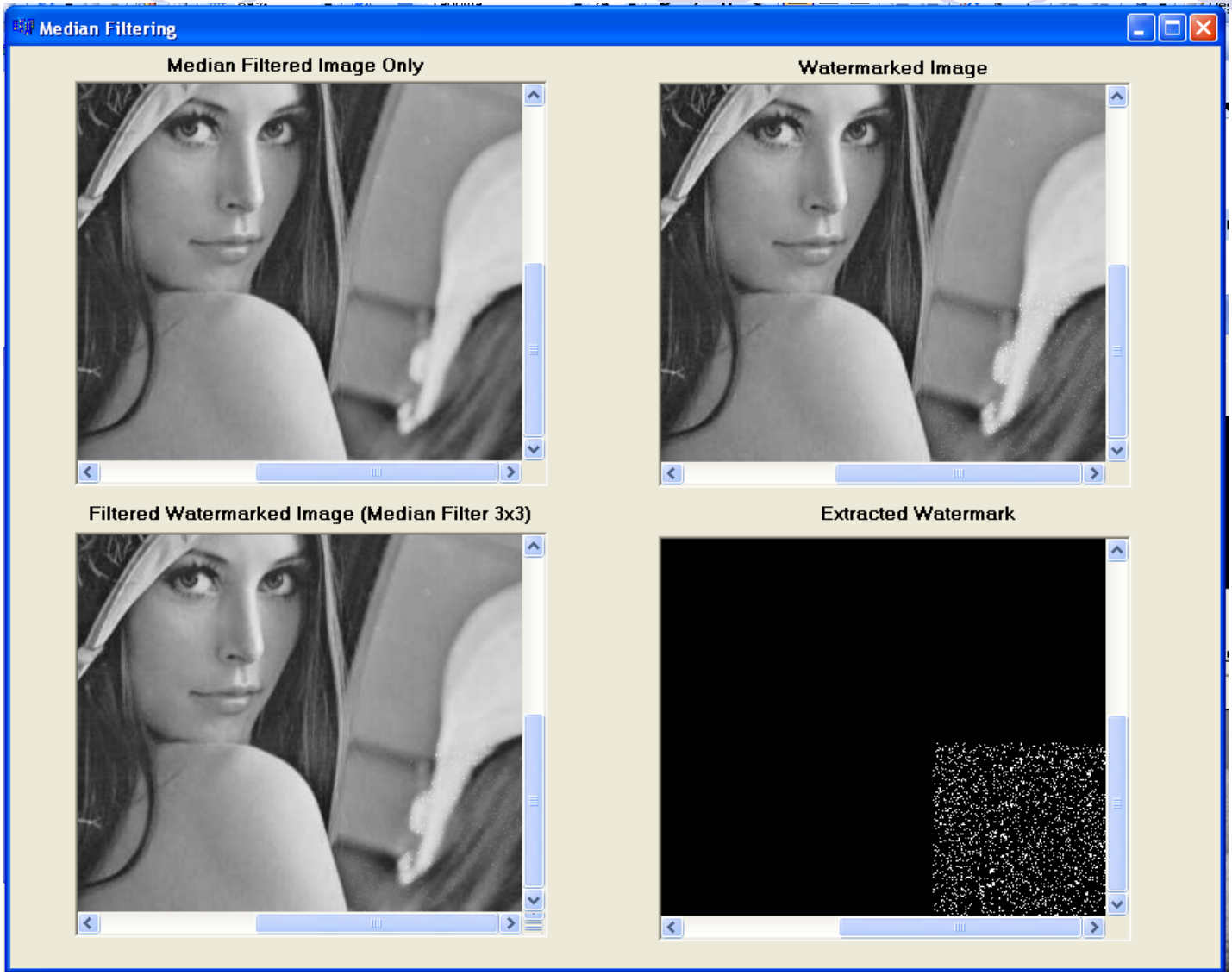
Results- Linear Lowpass Filter



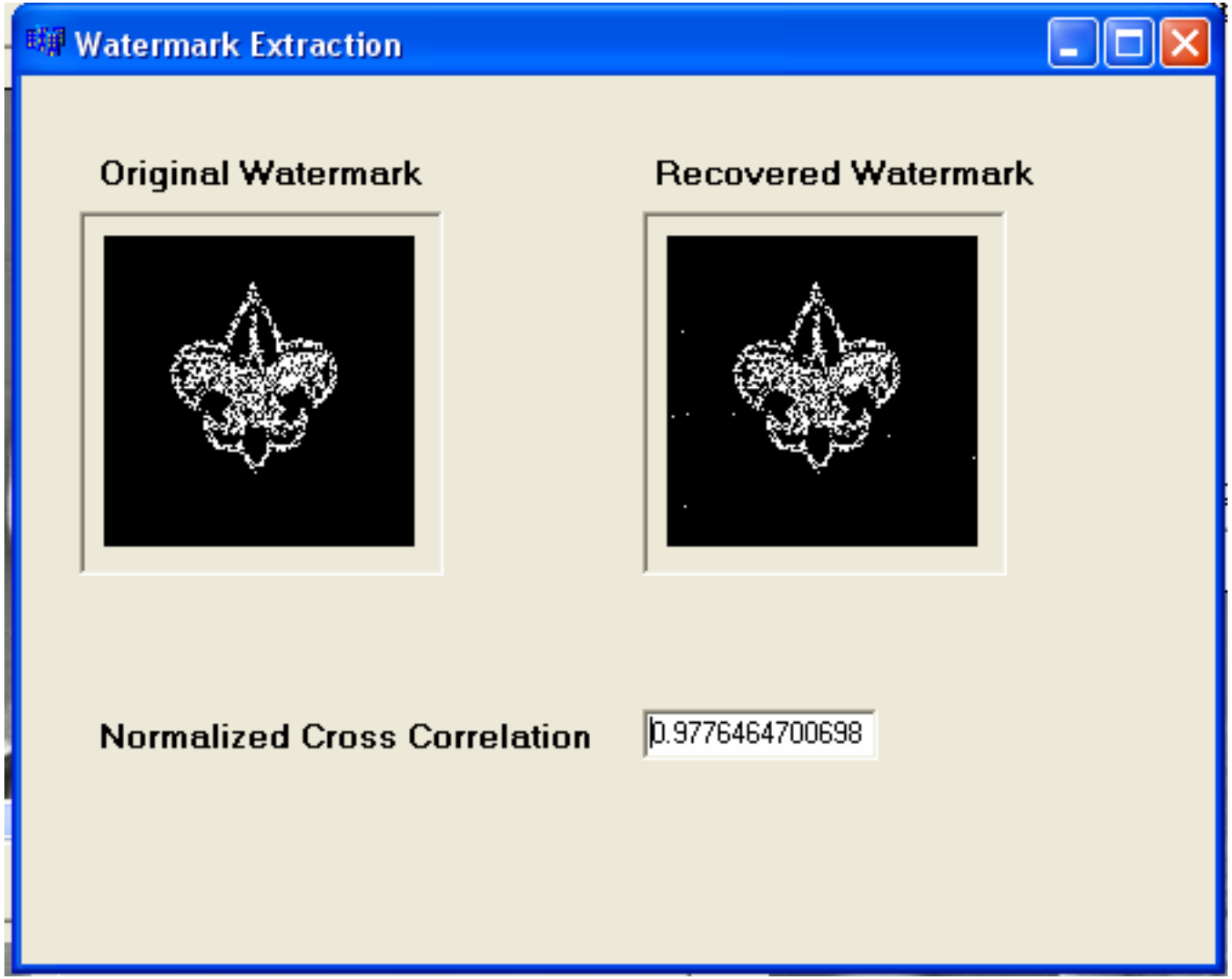
Linear Lowpass Filter-NC



Results- Median Filter



Median Filter- NC



Conclusions

- Extracted watermark can be easily used to identify the owner of the host image
- The proposed algorithm is robust to common image processing operations like linear lowpass and median filter.
- The proposed approach utilizes the sensitivity of HVS to adaptively modify the contents of the blocks.
- The pixel intensities are changed adaptively depending on the contrast of the block.

References

1. C-H. Lee, and Y-K. Lee, " An adaptive digital watermarking technique for copyright protection", *IEEE Transaction on Consumer Electronics,* Vol. 45, No. 4, pp. 1005-1014, 1999.

2. C.-T. Hsu and J.-L, Wu, "Hidden digital watermarks in images", *IEEE Transactions on Image Processing*, Vol. 8, No. 1, pp-58-68, 1999

3. M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification", *International conference on Image Processing,* Vol. 2, pp- 680-683, 1997.

4. C.-T. Hsu and J.-L, Wu, "Hidden Signatures in images", *Proceedings ICIP*, pp-223-226, 1996